Anti-money laundering and combatting the financing of terrorism (AML/CFT)

Guidance Notes for High-Value Goods Dealers (HVGDs)

Contents

1. Introduction/FAQ
2. Proceeds of Crime Act 2015
3. HVGD Risk Assessments
4. AML/CFT Policies, Controls & Procedures
5. Money Laundering Reporting Officers & Their Responsibilities
6. Customer Due Diligence & Assessing Risk
7. Ongoing Monitoring
8. Record Keeping, Data & Annual Returns
9. Employer & Employee Responsibilities
10. Potential High Value Goods Dealers
11. High Risk Dealers
12. Reporting Ownership & Management changes
13. Useful Contacts

Schedule 1 - How to Identify Customer ML/TF Risk
Schedule 2 - Glossary of Terms & Abbreviations

Notice

These guidance notes should be regarded as regulatory standards for the purposes of the Proceeds of Crime Act 2015 (POCA) and are issued pursuant to Section 11(3) of the Supervisory Bodies (Powers Etc.) Regulations 2017 (SBPR). Compliance with these guidance notes is enforceable pursuant to the provisions of POCA and of SBPR.

Issued: June 2017
Updated: April 2021
Version: 3.1

Office of Fair Trading • HM Government of Gibraltar • Suite 975, Europort • Gibraltar GX11 1AA
t (+350) 20071700 e oft@gibraltar.gov.gi w oft.gov.gi

1. Introduction/FAQ

1.1 What is AML/CFT?

AML/CFT stands for anti-money laundering and combatting the financing of terrorism. This refers to laws and systems designed to prevent money laundering and terrorist financing (ML/TF).

1.2 What is money laundering and terrorist financing (ML/TF)?

Money laundering is the process of transforming and concealing the profits generated by criminal activity and corruption (such as drug trafficking, market manipulation, fraud, tax evasion) into a 'clean'/legitimate asset.

The buying and selling of high value goods in cash is recognised as a major avenue for money laundering activity which is exploited by organised crime. Whereas high value goods transactions that are done via electronic payment can be easily tracked by law enforcement, transactions that involve large sums of cash are virtually invisible, making them very attractive to criminals seeking to launder illicit funds.

Terrorist financing is defined in section 1ZA of the Proceeds of Crime Act 2015 (**POCA**). It involves:

1. the use of funds or assets;
2. the making available of funds or assets; or
3. the acquisition, possession, concealment, conversion or transfer of funds,

for the purposes of terrorism. For more information about terrorist financing, and for Counter Terrorist Financing Guidance visit: www.gfiu.gov.gi/what-is-terrorist-financing.

The vulnerabilities and risks of money laundering and terrorist financing in Gibraltar are set out in the National Risk Assessment published by HM Government of Gibraltar (**NRA**). You can find a copy of the NRA in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

1.3 Why is the OFT issuing these guidance notes?

The OFT is responsible for ensuring that dealers in high value goods (see section 1.5) who receive large cash payments (see section 1.6) comply with their legal AML/CFT obligations as set out in the Proceeds of Crime Act 2015 (see section 2). It is issuing these guidance notes to assist these dealers to meet their obligations and to prevent ML/TF taking place through their trade in high value goods.

This guidance gives an overview of their legal obligations and explains how the OFT will supervise compliance. It also provides guidance to assist dealers in high value goods to identify high risk transactions and customers.

1.4 Are these guidance notes relevant to all cash payments?

No. Only to large cash payments for:

1. high value goods (see section 1.5),
2. which are above the monetary threshold (see section 1.5).

Furthermore, they do not apply to cash payments for tobacco either (see section 1.12).

1.5 What are high value goods?

A high value goods is:

1. any individual item; or

2. any good sold by weight or volume;

that is sold or is for sale by a business for a value which is equal to, or greater than, £2,000 (two thousand pounds). This includes any currency equivalents, based on the exchange rate at the time.

High value good ≥ £2,000

1.6 What is the monetary threshold?

The OFT will consider cash payments in any currency with a value which is equal to, or greater than, £8,000 (eight thousand pounds) as a large cash payment. This amount is referred to as the monetary threshold and includes any currency equivalents, based on the exchange rate at the time the transaction is made.

Monetary threshold = £8,000

1.7 Who do these guidance notes apply to?

These guidance notes apply to three types of dealers:

1. High-Value Good Dealers (**HVGDs**)

   Businesses that accept cash payments above the monetary threshold for high vale goods;

2. Potential HVGDs

   Businesses which are open to accepting cash payments above the monetary threshold for high vale goods, but have yet to receive such payments (see section 10); and

3. High Risk Dealers (**HRDs**)

   Businesses that, despite not receiving cash payments above the monetary threshold, sell high value goods that have a high ML/TF risk (see section 11).

The guidance notes also apply to the employees of the above-mentioned businesses.

1.8 Do these guidance notes apply to card payments and bank transfers?

No. They apply to payments in cash only, i.e. money in coins or notes.

1.9 Is the monetary threshold passed if cash is received over a period of time?

The monetary threshold is passed if the business receives:

1. a single cash payment of £8,000 or more;
2. a series of linked cash payments totalling £8,000 or more from the same customer (including payments on account); and/or
3. cash payments totalling £8,000 or more which appear to have been broken down into smaller amounts to fall below the £8,000 limit.

1.10 Is it prohibited to accept cash payments above the monetary threshold?

No. There is nothing wrong with accepting payments in cash above the monetary threshold.

Before doing so however, the business will be required to collect and record information about the buyer of the goods and to risk assess the client and/or the transaction (see Section 6 below). If, having done so, there is knowledge or suspicion that ML/TF will take place it must then report it (see sections 5.6 and 5.7).

1.11 Do all payments in cash above the monetary threshold need to be reported?

No. Only those payments which are connected to customers or transactions that, once risk assessed by the business, are known to be, or suspected of being, made in

connection with ML/TF (see 5.6 and 5.7 below).

1.12 Do these guidance notes apply to the sale of tobacco?

No. The supervisory authority for the trade in tobacco is HM Customs (see 12.3 below).

1.13 What are the obligations of HVGDs?

HVGDs' responsibilities include, but are not limited to:

1. Carrying out a risk assessment of their business's attractiveness and vulnerability to ML/TF (see Section 3 below);
2. Establishing appropriate policies and procedures commensurate to the business's risks to prevent the business being used to launder money or finance terrorism (see Section 4 below);
3. Appointing a money laundering reporting officer (**MLRO**) who understands the business's risks and responsibilities, its AML/CFT policies and who shall be responsible for all AML/CFT matters (see Section 5 below);
4. Carrying out risk assessments of its customers on a risk-based approach and keeping relevant documentation (see Section 6 below); and
5. Keeping appropriate AML/CFT records and submitting annual returns to the OFT (see Section 8 below); and
6. Training staff to ensure they are aware of ML/TF risks and of the business's AML/CFT polices (see Section 9 below).

For responsibilities of Potential HVGDs and HRDs see Sections 10 and 11 respectively.

1.14 What is the OFT's role?

As a Supervisory Authority under POCA (see Section 2 below), the OFT must effectively monitor HVGDs and take necessary measures to:

1. secure compliance by HVGDs with the requirements of POCA;
2. prevent such HVGDs from engaging or otherwise being concerned in (directly or indirectly) with ML/TF, or otherwise knowingly or recklessly assisting or facilitating such conduct by any other person;
3. identify and assess the ML/TF risk for HVGDs as set out in the NRA, a copy of which can be found on the OFT's website: www.oft.gov.giHVGD.

Furthermore, the OFT is required to report evidence of ML/TF to the Gibraltar Financial Intelligence Unit (**GFIU**).

1.15 How does the OFT monitor compliance by HVGDs?

The OFT risk assesses all HVGDs and HRDs compliance with their AML./CFT obligations based on:

1. documents submitted annually to the OFT, including:
    i. risk assessments (see section 3);
    ii. policies controls & procedures (see section 4); and
    iii. annual returns submitted (see section 6); and
2. regular onsite visits carried out by the OFT on all HVGDs and HRDs in order to ensure that they are meeting their AML/CFT obligations in practise.

The OFT also works closely with the Gibraltar Financial Intelligence Unit, law enforcement bodies and other AML/CFT supervisory authorities to monitor the market and uses various sources to acquire information and determine whether the

business is complying with their AML/CFT obligations or is being used for ML/TF.

1.16 Do these guidance notes contain all I need to know?

No. These guidance notes are for information purposes only so that HVGDs, Potential HVGDs, HRDs and their employees are given an overview of their legal obligations. For the definitive authority on your legal obligations regarding AML/CFT please refer to the Proceeds of Crime Act 2015 (see section 2).

1.17 Can I avoid the obligations in the Act and these guidance notes?

Yes. A dealer need not comply with parts of the Act or these guidance notes if:

1. they are not a High Risk Dealer (see Section 11 below);
2. they have a written policy not to accept cash payments above the monetary threshold; and
3. they have notified the OFT of their no cash policy.

2. Proceeds of Crime Act 2015 (POCA)

2.1 What is POCA?

POCA is a Gibraltar law aimed at preventing the abuse of the financial system for ML/TF and proliferation financing. It also sets out processes relating to the confiscation, investigation and recovery of the proceeds of unlawful conduct.

2.2 Where can I find POCA?

The full body of the Act may be found in the 'AML/CFT' page of the OFT's Website (www.oft.gov.gi) along with a pdf copy of these guidance notes.

It can also be found on the HM Government of Gibraltar's Gibraltar laws website (www.gibraltarlaws.gov.gi) by searching for "Proceeds of Crime".

2.3 Is all of POCA applicable?

All of POCA is applicable, however the most relevant part for HVGDs is Part III: 'Measures to prevent the use of the financial system for purposes of money laundering, terrorist financing and proliferation financing'. For ease of reference, HVGDs are defined as "relevant financial business" in section 9(1)(k) of POCA.

2.4 If I read these guidance notes, do I need read the Act?

Yes! These guidance notes only set out some of the most relevant provisions of POCA to the HVGD sector. These focus on ML/TF only as these are the criminal activities which HVGDs are most at risk of being exposed to and where the OFT has therefore focussed its guidance efforts. There are however other obligations in POCA that may not be referred to in this document, most notably in relation to proliferation financing.

You should not therefore regard this document as an exhaustive authority and should instead read it in conjunction with your legal AML/CFT obligations as set out in POCA.

2.5 What is proliferation financing (PF)?

PF refers to the act of providing funds or financial services which are used for the manufacture, acquisition, possession, development, transfer, stockpiling or use of

nuclear, chemical or biological weapons and their means of delivery. This is not an exhaustive definition and is indicative only.

HVGDs should understand PF and their obligations in relation to PF as set out in local and international legislation. For more information and guidance regarding PF please refer to the Counter-Proliferation Financing Guidance Notes on the GFIU's website: http://gfiu.gov.gi/uploads/docs/X86Ru_CPF_Guidance_Notes_v1.1.pdf .

3. HVGD Risk Assessments

3.1 What is a risk assessment?

Section 25A POCA sets out the requirement to risk assess their business. A risk assessment is the process of assessing the ML/TF risk that your business could be exposed to. Once the risks are understood appropriate systems and policies can be put in place to mitigate these risks (see section 4).

3.2 What do I need to consider when carrying out the risk assessment?

HVGDs must subjectively assess the relevant ML/TF risks to their business. When undertaking their risk assessment, the following questions should be considered:

1. Does the business understand how and why criminals may wish to launder illicit funds through the purchase of high value goods?
2. How does the business's:
   i. customer base;
   ii. type and value of goods traded; and
   iii. geographical area, impact its level of risk?
3. Are the business's customers buying for themselves or on behalf of a third party? Does the business know who these third parties are?
4. Does the business deal with any overseas sellers or buyers who are not local?
5. Does the business have systems in place to regularly monitor and detect any behavioural patterns or activities of its customers that could possibly be ML/TF schemes (see Schedule 1)?
6. Are the business's customer due diligence methods appropriate and sufficient to minimise the risk?(see Section 6).
7. Have the employees of the business received any training that might mitigate the risk of the business being used to launder illicit funds? (see section 9).

This list is not exhaustive and a risk based approach will require analysing the business's individual characteristics carefully.

For example, an international wholesale operation with overseas customers presents a very different risk profile to a high street jeweller in Main Street. However, both may be targeted by criminals if they have little or no AML/CFT controls in place. The environment in which a business is carried out affects the individual businesses' risk assessment. If a business has many high net-worth customers or deals with people from a particular country or region, this will influence the business wide assessment.

3.3 Is there more guidance to help my business carry out its risk assessment?

For detailed and specific guidance about carrying our risk assessments refer to the OFT's Risk Assessment Guidance Notes which can be found in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

The OFT has issued Dealers in precious metals and stones, diamonds and gold can find more in depth guidance on the risk-based approach to combatting ML/TF from the Financial Action Task Force through links in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

3.4 Ongoing obligations.

HVGDs have the responsibility of regularly conducting risk assessment as a means of focusing on risks specific to the business at that time and ensuring that AML/CFT systems and policies in place continue to be effective.

4. AML/CFT Policies, Controls & Procedures

4.1 Risk based policies, controls and procedures.

Pursuant to section 26 POCA, HVGD's must establish and maintain appropriate and risk-sensitive AML/CFT policies, controls and procedures. These policies, controls and procedures should protect the business and prevent it from being used as a tool for ML/TF.

All HVGDs must have a clear written AML/CFT policy based on the ML/TF risks associated to the specific business. These can be determined after carrying out a risk assessment of the business (see Section 3 above). The policy shall be proportionate to the nature and size of the HVGD.

The policy should contain well-defined controls and procedures to identify and manage the business's and its customers' ML/TF risks.

It must be made available to all employees of the business and to the OFT.

4.2 Who approves the policy?

Pursuant to section 26A POCA, the AML/CFT policy must be approved and adopted by the business's senior management who will include the board of director, executives and/or other senior managers.

4.3 What controls and procedures must be in place?

HVGDs must develop internal policies and procedures that allows it to:

1. assess the risk of their business being used by criminals for ML/TF (in accordance with Section 3);
2. carry out customer due diligence measures (see section 6) and monitor customers' business activities;
3. carry out ongoing CDD measures (see section7);
4. submit annual returns to the OFT (see section 8 below);
5. report suspicious clients or transactions to the GFIU where it suspects, or has reasonable grounds to suspect, that a transaction is related to ML/TF (see section 5.8);
6. keep customer, transactional and staff training records (see section 9);

7. ensure employees:
    i. are aware of POCA and these guidance notes;
    ii. are aware of the business's AML/CFT policy;
    iii. have the necessary training; and
    iv. report suspicious activity to the MLRO (see section 9.4).

A complete list of the legal requirements are set out in section 26 POCA.

HVGDs must also ensure they have the necessary management control systems in place and the required resources to implement the policy.

4.4 What if I have multiple businesses?

Pursuant to section 26 (1B) POCA, AML/CFT policies and procedures should be applicable to all the business in the same group, and should be appropriate to each of the business.

Group AML/CFT policies and procedures should allow for sharing information required for the purposes of CDD and the assessment and management of ML/TF risk by all the group's businesses. The MLRO of each business in the group should be provided with customer, and transaction information from the other businesses when necessary for AML/CFT purposes. Adequate safeguards on the confidentiality and use of information exchanged should be in place. Refer to the full set of requirements in Section 26(1B) POCA.

If you have branches and subsidiaries outside of Gibraltar you should note the requiems of Section 21 POCA.

4.5 Do I comply fully once I have a policy?

It is important that the policy is put into operation. If a HVGD has the best policy in the world, but it is not used or it is not appropriate to their business, then it is of no use and the HVGD will not be meeting its AML/CFT obligations.

It must therefore be based on the findings of the business's risk assessment (see section 3) and be made readily available to all employees who should be trained about how to implement it (see section 9 below). A copy of the policy must also be provided to the OFT.

Pursuant to section 26(1A) POCA HVGD's must also undertake an independent audit function for the purposes of testing their AML/CFT policies, controls and procedures and ensure they are appropriate.

4.6 Undertaking an audit

Audits must have regard to the nature and size of the HVGD (section 26(1A) POCA) and should happen at regular intervals or where a deficiency with the business's AML/CFT policy, controls or procedures is identified. The frequency and scale of the audit shall be proportionate to the size and nature of the business as well as findings and recommendations from previous audits and any other relevant AML/CFT considerations.

Audits must be independent but there is no requirement to engage the services of a third party in order to carry out this function. It can also be performed by a person from within the business. Whoever carries out the audit the HVGD must ensure their independence. The auditor must not:

1. have been involved in carrying out the HVGD's risk assessment;
2. have been involved in the development of the HVGD's AML/CFT policies, controls and procedures; and/or

3. be involved in applying the HVGD's AML/CFT policies, controls and procedures.

The person must provide an independent, objective and impartial view on the efficacy of the policies, controls and procedures. It is the responsibility of the business to determine the independence of the individuals and this should to be evaluated at least annually.

The HVGD must also ensure that the person conducting the audit has sufficient knowledge of the HVGD's AML/CFT obligations to assess the efficacy of the business's policies, controls and procedures.

4.7 Do I need a policy if I work alone?

Yes. You must implement a policy, however this need not be in writing until you are working with someone else. If not in writing you must be able to explain to the OFT upon request:

1. your business's ML/TF risks and vulnerabilities;
2. your business's AML/CFT policies, controls & procedures to mitigate those risks.

5. MLROs & their responsibilities

5.1 What is an MLRO?

All HVGDs must nominate a money laundering reporting officer (**MLRO)**.

MLROs must be registered with the OFT by completing and submitting an MLRO nomination form. The form is available to download in the 'AML/CFT' section of the OFT'S website: www.oft.gov.gi.

5.2 Who must be appointed MLRO?

A MLRO must be director, senior manager or partner of the business. They play an important role, so they must be someone who:

1. can be trusted with the responsibility;
2. has access to all customer files and records;
3. can give necessary instructions to other employees; and
4. is autonomous enough to decide whether they need to report suspicious activities or transactions.

If you work alone, you are the MLRO.

5.3 What is the MLRO's role?

The MLRO is generally responsible for dealing with any AML/CFT matters and is the OFT's liaison for the business.

They must carry out appropriate risk assessments of the business and its customers (in accordance with Sections 3 and 6 respectively) and ensure all AML/CFT policies and procedures are adhered to and understood by all employees (see sections 4 and 9).

The MLRO must also be aware of daily transactions and monitor any suspicious activities involving the business that might be linked to ML/TF. Where necessary the MLRO must report such activities or risks to the GFIU by submitting a Suspicious Activity Report (**SAR**) (see 5.8 below). Where a HVGD suspects, or has reasonable grounds to suspect, that a transaction is related to ML/TF it is required to report it promptly to the GFIU. This includes attempted transactions whether or not these are below the monetary threshold.

5.4 What are the MLRO's responsibilities?

MLROs must receive reports of suspicious activity from any employee in the business. They must then evaluate the reports for any evidence of ML/TF and carry out an appropriate risk assessment based on the report and the customer's due diligence records.

The MLRO may also be responsible for other tasks to ensure the business complies with POCA, e.g:

1. putting in place and operating AML/CFT controls and procedures (Section 4 above);
2. training staff in preventing ML/TF within the business;
3. keeping records of customer due diligence and risk assessments (see 7.1 below); and
4. ensuring the HVGD's workers are not part of a ML/TF scheme.

5.5 How does a MLRO identify ML/TF risk?

The MLRO must consider all of the information about the customer, business relationship and the transaction which is intended to be carried out. If the MLRO knows, suspects or has reasonable grounds to suspect that a person is engaged, or is attempting to, launder money or finance terrorism they must report this to the GFIU at the earliest possible opportunity using a SAR (See 5.8 below).

5.6 What is meant by 'knowledge'?

A MLRO has 'knowledge' if they actually know something to be true. The MLRO may however infer this from surrounding circumstances, including the due diligence process and by asking questions.

If in doubt, the MLRO should seek clarification or ask for evidence from the person to support their evaluation.

5.7 What constitutes suspicion?

Suspicion must be assessed both subjectively and objectively. It must extend beyond mere speculation and must be based on some foundation. To be suspicious MLROs must have a degree of satisfaction that ML/TF may be taking place which, does not necessarily amount to knowledge (see 5.6 above), but at least extends beyond speculation.

If in doubt, the MLRO should seek clarification or ask for evidence from the suspected person to support their evaluation.

5.8 How does the MLRO report to the GFIU?

For more information about how to do this visit https://www.gfiu.gov.gi/reporting. This will allow the MLRO to sign up to the GFIU's Themis online system.

Alternatively, reports may be made to the GFIU by completing a downloaded Suspicious Activity Report form and submitting it to the GFIU by e-mail (gfiu@gcid.gov.gi) or delivered by hand to their offices at Suite 832, Europort. The form can downloaded from the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

5.9 What happens once a SAR has been submitted?

Once a SAR is submitted the MLRO must ensure the transaction does not take place. The GFIU has fourteen days to assess the information submitted in the SAR and reach a decision about how to proceed. They may seek further information from you.

At the end of the fourteen days if you have not received any further notice from the GFIU then nothing further is required, the transaction may take place.

5.10 Should the suspicious transaction be allowed to go ahead?

No. The MLRO must seek consent from the GFIU before proceeding with a transaction it suspects is being carried out to launder money or finance terrorism.

5.11 Should the person being reported be made aware of their report?

No! It is a criminal offence for anyone to say or do anything that may prejudice an investigation or 'tip off' another person that a suspicion has been raised, a SAR has been submitted or that a money laundering or terrorist financing investigation may be carried out. It is also an offence to falsify, conceal or destroy documents relevant to investigations.

Nobody should tell or inform the person involved in the transaction or anyone else that:

1. the transaction is being or was delayed because a suspicion has been raised;
2. details of a transaction have or will be reported to the GFIU; or
3. law enforcement agencies are investigating the customer.

Where a MLRO forms a suspicion of money laundering or terrorist financing, and they reasonably believe that applying CDD measures (see Section 6 below) will 'tip-off' the customer, then the MLRO should not apply such measures and instead submit a SAR.

5.12 Tipping off through CDD measures

Pursuant to section 11(5A) POCA, where, during the course of applying customer due diligence measures (see section 6 below), a HVGD knows, suspects or has reasonable grounds to suspect that the person subject to such measures or another person is engaged in ML/TF or proliferation financing, or is attempting any one or more of those acts, the HVGD must, where it is of the opinion that to continue would result in the tipping-off of the person, cease applying customer due diligence measures, and shall make a relevant disclosure to the GFIU without delay.

5.13 Sanctions

Sanctions are legal restrictions imposed by the United Nations, European Union, United Kingdom or Gibraltar against states, people, businesses, organisations and financial institutions in appropriate cases to achieve specific international policy or security objectives.

It is an offence under section 9 of the Sanctions Act 2019 to breach, or to assist a breach, of an international sanction. You are not therefore allowed to deal with persons subject to a sanction unless you have a licence, permit or other authorisation to do so issued in accordance with Section 10 of the Act.

The Act requires HVGDs to have policies, controls and procedures in place to check all of its customers on the international sanctions lists. Furthermore, HVGDs must ensure that appropriate ongoing checks are carried out on both new and existing clients as and when the sanctions lists are updated.

For more information refer to the 'Sanctions' section of the GFIU's website (www.gfiu.gov.gi/sanctions) where you will have access to the GFIU's Financial

Sanctions Guidance Notes and to the sanctions lists.

The full body of the Act may be found in the 'Documents' section of the 'AML/CFT' page of the OFT's Website (www.oft.gov.gi).

5.14 What happens in the MLRO's absence?

A MLRO's duties can be temporarily delegated to someone else. This does not relieve the MLRO of their responsibility. A deputy or alternate may only be appointed during periods of absence.

A MLRO's absence should not restrict the HVGD's ability to monitor risk and submit SARs to the GFIU.

5.15 Is there more guidance for MLROs?

The GFIU has produced AML/CFT guidance notes on SARs for MLROs & Reporters. To access to this document please contact the GFIU or request a copy via email: admin@gfiu.gov.gi. For more information visit the GFIU's website: https://www.gfiu.gov.gi/reporting.

6. Customer Due Diligence & Assessing Risk

6.1 What are customer due diligence measures?

Customer due diligence (**CDD)** measures (also known as 'know your customer' or KYC) refer to processes whereby a business carries out checks on its customers to establish who they are and to understand the purpose of the transactions they want to carry out. This allows the business to determine whether there is a risk that they are linked to ML/TF. A full definition of CDD measures is set out in Section 10 of POCA.

CDD measures involves:

1. identifying the customer and establishing who they are;
2. understanding the ownership and control structure of the customer, including identifying customers' beneficial owners (see section 6.5);
3. understanding and obtaining information on the purpose and intended nature of the business relationship or occasional transaction;
4. taking a risk-based approach to the verification of the identity of the customer and all beneficial owners (see section 6.3)
5. determining whether the customer, or its beneficial owner, is a politically exposed person (see section 6.12);
6. taking a risk-based approach to the verification of the source of funds and the source of wealth of the customer and beneficial owners; and
7. understanding the ownership and control structures of customers that are corporate or legal entities, trusts, foundations and other legal arrangements.

CDD therefore involves collecting documentation and information to allow the business to understand who it is dealing with, what the transaction is about and who is benefiting from the transaction. This in turn allows the business to carry out a ML/TF risk assessment of the customer before selling their high value goods to them.

6.2 When are CDD measures carried out?

CDD must be performed before any financial transactions take place.

Pursuant to section 11(1) and 13(2) POCA, HVGDs must apply CDD measures and verify the identity of the customer (and any beneficial owner (see section 6.5)) before:

1. it sells high value goods, or any other goods (POCA section 11(1)(ba)), in cash above the monetary threshold, whether the transaction is carried out in a single operation or in several operations which appear to be linked (see section 1); and/or
2. it establishes a business, professional or commercial relationship with a customer which is expected, at the time when contact is established, to have an element of duration.

HVGDs must also apply CDD measures where it suspects ML/TF or proliferation financing in any circumstances, regardless of whether the payment for goods is in cash and/or surpasses the monetary threshold.

HVGDs are also required to carry out ongoing monitoring and due diligence of existing business relationships (see section 7).

6.3 What are my CDD obligations?

HVGDs must undertake sufficient monitoring of the transactions and business relationships they enter into to enable the detection of unusual or suspicious transactions.

Pursuant to section 11(3) and (5) POCA, a HVGD must determine the extent of CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. In doing so the HVGD must at least, take into account the following list of risk variables:

1. the purpose of the relationship or transaction;
2. the size of the transactions undertaken; and
3. the regularity or duration of the business relationship.

The HVGD must also be able to demonstrate to the OFT that the extent of the measures is appropriate in view of the risks of ML/TF that have been identified.

6.4 Who needs to be checked?

Appropriate CDD must always be completed on customers wishing to purchase high value goods above the monetary threshold either in one, or multiple, related transactions (see section 1.9).

The identity of the Customer must be known and their identity must be verified through appropriate original documentation.

Similarly, the identity of any ultimate beneficial owner must be known and verified (see section 6.5).

Due diligence is not required for banks, EU listed companies or Governmental entities.

HVGDs must apply ongoing CDD measures to business relationships (see section 7).

6.5 What is a beneficial owner (BO)?

The definition of 'beneficial owner' is set out in section 7(1A) POCA.

A BO is an individual (or 'natural person') who will ultimately benefit from a transaction or business relationship.

Where an individual is conducting a transaction or activity for their own benefit

then they are the beneficial owner (POCA section 7.(1A)(a)(i)).

If, however, a transaction is being carried out by a customer on behalf of another person then the BO is the individual

1. on whose behalf a transaction or activity is being conducted (POCA section 7.(1A)(a)(ii)); and/or
2. who ultimately owns or controls the customer entering into the transaction.

Where a HVGD's customer is entering into a transaction on behalf of another person the HVGD must identify and verify who that other person is. That person is the BO.

Broadly speaking where an individual either owns or has control over 25% of a company or is a settlor, trustee, protector or beneficiary of a trust (or similar) that is the HVGD's customer, that individual will be a BO.

For detailed and specific guidance about BOs and how to identify them refer to the OFT's Beneficial Ownership Guidance Notes which can be found in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

Pursuant to section 11(4A) POCA, where a HVGD is required to apply CDD measures to a trust, corporate or legal entity it shall collect proof of registration (or an excerpt) of the BO's registration on the Gibraltar Register of Ultimate Beneficial Owners (https://uboregister.egov.gi).

6.6 What happens if I have difficulties or am unable to collect CDD?

In relation to companies, you must exhaust all possible means to determine who its BO is. This will involve making appropriate and proactive enquiries. You must be able to demonstrate the efforts made to do so to the OFT.

However, if after having exhausting all possible means:

1. there is doubt as to who the BO is; or
2. no person is identified as the BO,

then the BO shall be the individual exercising control over the company via other means (POCA s7(c)(ii)).

If, after having exhausted all possible means, there is still doubt about who the individual exercising control is, then the BO shall be the individual who holds the senior management position in the customer (POCA s7(c)(ii) & (iv)).

More generally, pursuant to section 15(1) POCA, if any person or entity is unable or unwilling to submit the relevant CDD documents requested and the HVGD is unable to carry out appropriate CDD measures it should not proceed with the transaction and, where applicable, it must terminate the business relationship. If the relationship is not terminated this should be recorded.

Furthermore, the HVGD must submit a SAR to the GFIU in relation to the customer (see paragraphs 5.8 to 5.10 above).

HVGDs should keep a record of any difficulties encountered during the CDD process (POCA section 10(l)).

HVGDs are prohibited from carrying out transactions above the monetary threshold for anonymous customers or customers which have provided aliases or fictitious names.

6.7 Applying CDD measures.

CDD measures allow a HVGD to assess a customer's AML/CFT risk and whether a

transaction may proceed without a real risk of the HVGD being involved in a transaction which is intended to launder money or finance terrorism.

The level of CDD required will depend on the ML/TF risk posed to the business by the customer and the transaction. The risk must be assessed by considering the identity of the customer, the type of goods being purchased and any other information or concerns the business may have about the customer or transaction.

The identity of Customers should be verified on the basis of original documents, data or information obtained from reliable and independent sources.

CDD however goes beyond simply carrying out identity checks. People which are well known to the business may become involved in illegal activity e.g. if their personal circumstances change or they face some new financial pressure. CDD measures should reduce this risk and the opportunities for staff to be corrupted.

A low AML/CFT assessment will require a simplified due diligence process and a high risk transaction or customer will require an enhanced due diligence process with medium risks requiring elements of both depending on the risk. For guidance on how to identify ML/TF risks see Schedule 1.

6.8 Low risk customers: Simplified CDD measures.

Pursuant to section 16 POCA, where a HVGD, having applied CDD measures:

1. identifies areas of lower risk;
2. has ascertained that the business relationship or the transaction presents a lower degree of risk; and
3. has not identified a suspicion or knowledge of ML/TF, or proliferation financing,

it may record the reasons why it perceives a reduced risk and apply simplified CDD measures. For guidance on how to identify low risk customers see Schedule 1.

Simplified CDD can include, but may not be limited to, collecting the following basic information:

Individuals:

1. Full Name;
2. Date of Birth;
3. residential address;
4. a copy of the customer's original Passport/ID (or any other Government-issued photographic document); and
5. the customer's source of income or wealth (e.g. employment)

Companies:

1. an up to date company profile issued by Companies House or the following corporate documents:
   i. Certificate of incorporation;
   ii. Register of Members; and
   iii. Register of Directors; and
2. the address of the registered office and, if different, a principal place of business.

Where a transaction involves a trust (or other similar legal arrangement) you must collect a copy of the trust deed (or other similar legal document) establishing and setting out the nature of that arrangement.

HVGDs must keep copies of due diligence documents (see Section 7 below).

6.9 High risk customers: Enhanced CDD measures.

HVGDs must apply enhanced CDD measures to appropriately manage and mitigate risks when dealing with -

1. customers identified as being high risk (see Schedule 1, paragraph 3);
2. natural persons or legal entities established in third countries identified by the European Commission as high risk third countries; and
3. politically exposed person, or their family members and close associates (see 6.10 below); and
4. in other circumstances as set out in Section 17(1) POCA.

For guidance on how to identify high risk customers see Schedule 1.

When dealing with high risk customers it is important to perform enhanced due diligence as a result of the increased risk of ML/TF. MLROs must keep records as to why, in their view, the need for enhanced CDD is appropriate to the risk posed by the business relationship.

Examples of enhanced CDD:

1. A copy of the customer's Passport/ID which is certified as true copy of the original by a third party professional;
2. Proof of the customer's address provided in a document such as a utility bill or bank statement;
3. Proof of the customer's and the beneficial owners' source of funds and source of wealth commensurate to the transaction; and
4. Additional information on:
    i. the customer and on the beneficial owners;
    ii. the intended nature of the business relationship;
    iii. the reasons for the transactions.

HVGDs must also apply specific enhanced CDD measures in relation to:

1. business relationships or transactions involving high-risk third countries as set out in section 17(6) POCA; and
2. politically exposed persons as set out in section 20 and 20B POCA (see section 6.12).

HVGDs must obtain the approval of senior management for establishing or continuing a business relationship with a customer requiring enhanced CDD.

HVGDs must keep copies of due diligence documents (see Section 7 below).

6.10 What am I looking for?

CDD documentation, along with all other surrounding factors and information about the customer and the type of transaction. HVGDs are also required to understand the nature of their customer's business and its ownership and control structure.

This information will permit the HVGD's MLRO to assess the AML/CFT risk posed and whether to report suspicious activity to the GFIU.

Some examples of suspicious activity specific to HVGDs include occasions where a customer:

1. appears unwilling to submit any identification documents;
2. seems uninterested in the value of the good nor viewing and inspecting the goods before purchase;
3. acquires several high value goods within a short period of time which are ordinarily only bought once by other customers;

4. requests information from the business reference its AML/CFT policies; and
5. wishes to make the payment through a company without explanation.

For more guidance on ML/TF risks please see Schedule 1.

6.11 Non face-to-face transactions

Pursuant to Section 18 POCA, Where the customer has not been physically present for identification purposes, HVGDs must take specific and adequate measures to compensate for the higher risk. This may for instance include:

1. ensuring that the customer's identity is established by additional documents, data or information;
2. applying measures to verify or certify the documents provided, e.g. requiring a third party professional with AML/CFT expertise to certify them e.g. a lawyer.

Where this is not possible HVGDs should not accept cash and instead only accept a card payment or bank transfer.

6.12 Politically exposed persons.

A politically exposed person (**PEP**) is a person who is or has been entrusted with a prominent public function locally or internationally (see definition on paragraph 4 of Schedule 1). These individuals are at a higher risk of being connected to ML/TF due to the position and influence they hold and because they can be susceptible to corruption.

Pursuant to section 26(2)(c) POCA a HVGD must have policies, controls and procedures in place HVGD to determine whether a customer or the BO of a customer is a PEP, a PEP's 'family member' or 'a person known to be their close associate' (as defined in Section 20A POCA). Given Gibraltar's small size and the closeness of its community, this is potentially a large group of persons and this may therefore make it easier for these persons to be identified.

Pursuant to section 20 POCA, before entering into a transaction with a PEP, a PEP's family member, a PEP's close associate or a customer whose BO is a PEP, the HVGD must:

1. carry out enhanced due diligence (see 6.9 above);
2. have approval from senior management;
3. take adequate measures to establish the source of wealth and funds which are involved in the existing or proposed transaction.

Section 20B POCA also sets out the additional continuing obligations with regard to PEPs.

For in depth guidance on PEPs please refer to the FATF's guidance which can be found in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

6.13 Risk assessments

HVGDs are required to keep a written risk assessment in respect of every transaction (or a series of linked transactions, see 1.9 above) above the monetary threshold and the action taken in respect of any suspicious activity detected.

The OFT encourages all HVGDs to keep a risk assessment file as they must be able to demonstrate to the OFT that the extent of the CDD measures it has applied is appropriate to the client and the transaction in view of the risks of ML/TF that have been identified. Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution or criminal activity.

6.14 Can I rely on someone else's due diligence?

If a HVGD is satisfied that a third party has already carried out appropriate CDD measures on its customers, they may rely on that CDD as long as they are satisfied that:

1. the CDD measures are appropriate to the customer's level of risk as assessed by the HVGD; and
2. the CDD measures are current and up to date.

Copies of the CDD documentation must be provided by the third party to the HVGD. The HVGD is required to carry out its own risk assessment on the customer based on the CDD documentation received prior to the HVGD selling high value goods to the customer. It is not possible for the HVGD to rely on the third parties' risk assessments!

The responsibility to carry out CDD measures, to risk assess and to keep records on its customers shall always ultimately remain with the HVGD.

6.15 When do I report suspicious activity?

This will depend on the risk assessment carried out and is ultimately a question for the MLRO, having considered all information it has about the customer and the transaction through the CDD measures.

It should be made where the MLRO has either knowledge (see 5.6 above) or is suspicious (see 5.7 above) that ML/TF is or may be taking place.

If in doubt, submit an SAR! (see sections 5.8 to 5.10)

6.16 Tipping off

Pursuant to Section 11 (5A) POCA where, during the course of applying CDD measures, the HVGD knows, suspects or has reasonable grounds to suspect that the person subject to such measures or another person is engaged in ML/TF or proliferation financing, or is attempting any one or more of those acts, the HVGD must, where it is of the opinion that to continue would result in the tipping-off of the person, cease applying CDD measures, and shall make a relevant disclosure to the GFIU without delay.

6.17 Ongoing monitoring

Where HVGDs have ongoing business relations with its customers they HVGDs are required to carry out ongoing monitoring of these existing business relationships (see section 7).

6.18 Records.

HVGDs must keep copies of the documents requested while conducting CDD procedures along with all relevant documents appertaining to the business relationship (see Section 8 below).

7. Ongoing Monitoring

7.1 Ongoing monitoring

HVGDs are required to carry out ongoing monitoring and due diligence of existing business relationships. This requirement is set out in sections 11(2) and 12 POCA.

7.2 What are business relationships?

It means a business, professional or commercial relationship which is connected with the HVGD's activities and which is expected, at the time when contact is established, to have an element of duration.

Ongoing monitoring does not apply to occasional, one-off transactions. It may however apply to customers who have been sold goods above the monetary threshold or high value goods in cash more than once or on an ongoing basis.

7.3 What does ongoing monitoring involve?

Ongoing monitoring means:

1. scrutinising transactions undertaken throughout the course of the relationship to ensure that they are consistent with the HVGD's knowledge of the customer, their business, their risk profile and their source of funds; and
2. undertaking reviews of existing records (and updating these where necessary) to ensure that the documents, data or information obtained for the purpose of applying CDD measures is kept up-to-date and relevant.

HVGDs must determine the extent of ongoing monitoring on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. You must be able to demonstrate to the OFT that the extent of the measures is appropriate in view of the risks of ML/TF that have been identified.

7.4 When do I need to do this?

Ongoing monitoring must be carried out at regular intervals. As an indicator the OFT would expect that:

1. high risk business relationships are reviewed at least every year;
2. medium risk business relationships are reviewed every two year; and
3. low risk business relationships are reviewed every three years.

These time frames are indicative only and you must adapt your ongoing monitoring to your business's and the customer's risk as determined and recorded by your business.

When dealing with high risk transactions or customers requiring enhanced CDD, HVGDs must conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Further monitoring and CDD measures must also be carried out when the relevant circumstances of a customer change. When this occurs the HVGD must apply CDD measures to the existing customer on the basis of materiality and on a risk sensitive basis (POCA section 11(2)(a))

7.5 When do the relevant circumstances of a customer change?

Any material change to a customer will trigger the need for a HVGD to reapply CDD measures. A material change is one which would require a reasonable HVGD to reassess the ML/TF risk of the business relationship in light of those changes. There is no exhaustive list for what a material change is, however material changes can include:

1. a change in the nature or regularity of the transactions carried out by the business (See Schedule 1, paragraph 5, patterns of business); or
2. a change to the ownership or management of the customer.

HVGDs should not just take into consideration the risk profile of the existing customer but also the impact that that customer's business may have on the HVGD as a whole. For example, a customer may be considered low risk but their business

represents a substantial part of the HVGD's turnover. A trigger event that would not be material for smaller customers may be material for a HVGDs large customers, triggering the need apply CDD measures once again.

Applying a risk based approach, HVGDs should take into consideration the evolving risk profile of existing customers when assessing their AML/CFT risk. While customers with a consistent risk profile are not exempt from ongoing CDD measures, resources should be focussed on those which are more recent, or those with changes in the pattern of spending or the types of goods they are interested in.

8. Record Keeping, Data & Annual Returns

8.1 What records must be kept?

HVGDs must keep records and data about:

1. cash transactions above the monetary threshold and business relationships (section 8.2 and 8.3);
2. cash transactions of high value goods equal to or above £2,000 (section 8.4); and
3. staff training (section 9.3).

The records and data must be readily available for inspection by the OFT on request.

8.2 Transactions above the monetary threshold and business relationships

HVGDs' general record keeping obligations are set out in section 25 POCA. All HVGDs must have appropriate systems in place for recording and storing:

1. a copy of the documents and information collected while applying CDD measures (see section 6);
2. the supporting evidence and records of all transactions (or set of series of linked cash transactions) above the monetary threshold (see section 8.3);
3. the written risk assessment of every transaction (or set of related transactions) above the monetary threshold and every business relationship (see section 6.13); and
4. the action taken in respect of any suspicious activity detected (see sections 5.5 to 5.7).

In addition, HVGDs must also keep the records of any difficulties encountered during the CDD process (POCA section 10(l)).

8.3 What type of data must be collected about these transactions?

As much data and information as you can about the transactions, including account files and correspondence, as well as any other information that may reasonably be necessary to identify such transactions. The evidence and records must be sufficient so as to permit the reconstruction of individual transactions so as to provide evidence for the prosecution of criminal activity where necessary (Section 25 (2A) POCA).

Every transaction should have a detailed invoice specifying:

1. a description of the good(s) sold;
2. the quantity of the goods sold, by unit or otherwise (e.g. weight);
3. the relevant serial number for the goods;

4. the full name of the person purchasing the goods as stated in their passport/ID;
5. the cash paid in exchange for the goods;
6. an identifying reference for the goods to the HVGD's stock records; and
7. account files and business correspondence where relevant.

You must also keep sufficient data to allow you to complete and submit an Annual Return to the OFT (see section 8.6).

8.4 Transactions of high value goods

The OFT requires all HVGDs to collect the following data in relation to every cash transaction above £2,000 for any high value goods (see section 1.5):

1. a detailed description of the good(s) sold;
2. the quantity of the goods sold, by unit or otherwise (e.g. weight);
3. the relevant serial number for the goods;
4. the full name of the person purchasing the goods as stated in their passport/ID;
5. the cash paid in exchange for the goods; and
6. an identifying reference for the goods to the HVGD's stock records.

This may be kept in the form of a detailed invoice.

When dealing with the high risk goods listed in section 11.2, HVGDs must regard all transactions in cash for these high risk goods by a person, or group of associated persons, as a series of linked cash transactions for determining whether they cumulatively go above £2,000.

8.5 How long must I keep the records for?

HVGDs must keep these records for inspection for five years after the date of the relevant transaction or the date when staff training was delivered (Section 25(3) POCA).

8.6 What will the records be used for?

The OFT may use it powers to request copies of the HVGD's records and data at any time. HVGDs should be able to provide the records and data to the OFT swiftly.

HVGDs are also required to review their CDD records in accordance with ongoing requirements of section 12(2)(b) POCA (see 7 above).

Additionally, HVGDs are required to submit information annually to the OFT in advance of the renewal of the business licence and may be required to submit an annual returns to the OFT providing information and data about cash transactions above the monetary threshold during that year (see section 8.7). This information should correspond with the HVGD's records.

The annual return form can be found in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

8.7 When are the Annual Returns due?

Pre 2021-22 reporting period:

This shall be the same day as the due date for submission of accounts and tax returns by the HVGD to the Income Tax Office.

If the HVGD is a company, the Annual Return is due nine months after the HVGD's financial year end. If the HVGD is a sole trader it is due on 30th November of each year.

Reporting period from 2021-22 going forward:

A new system is being introduced for the 2021-22 reporting period going forward.

Prior to the renewal of their business licence after 1st January 2021, HVGDs will receive a business licence renewal notice which shall require them, as part of the renewal process, to declare whether or not they have received payments in cash above the monetary threshold during the licensing term which is due to expire. Where they declare that that they have, the HVGD will have to complete and submit the new HVGD Annual Return containing up to date financial and other data for the licence term which is due to expire. The due date shall be three months after the HVGD's business licence renewal date.

8.8 What if I miss the deadline?

We strongly urge that you take the appropriate steps to ensure that your business submits its annual returns on time. Failure to do so may result in the HVGD not being allowed to renew their business licence. They may also be subject to enforcement action by the OFT that may include:

1. a fine,
2. the suspension or revocation of their business licence; and/or
3. temporary bans for persons in managerial positions.

8.9 What will the OFT do with the Annual Return?

The information will allow the OFT to:

1. collect data about the amount and type of high value transactions carried out by the HVGD and more generally in Gibraltar;
2. monitor HVGDs' compliance with their obligations under POCA and these guidance notes; and
3. identify suspicious trends and ML/TF schemes .

This data will also help the OFT analyse each HVGD on a risk based approach to determine the likelihood of the HVGD being targeted by criminals.

The OFT may carry out onsite visits and seek information from HVGDs in relation to the information contained in annual returns to ensure that these are being completed accurately. The OFT may also request HVGDs records to examine and investigate any suspicious activity.

The failure by a HVGD to submit an annual return is automatically considered as non-compliance by the OFT.

The data may be provided to other AML/CFT supervisory authorities and law enforcement bodies as permitted under the law.

9. Employer & Employee Responsibilities

9.1 What are my responsibilities as an employer?

HVGDs must ensure that they have screening procedures to ensure high standards when hiring employees.

Additionally, employers have a duty to ensure that its employees have sufficient training to help them both recognise and report potential ML/TF. Staff must be made aware and understand the following:

1. what money laundering and terrorist financing is;
2. the laws concerning AML/CFT, including POCA, and the requirements in these guidance notes;
3. the ML/TF risks to which the trade sector generally is exposed;
4. the specific ML/TF risk to which the HVGD is exposed (see section 3);
5. the HVGDs AML/CFT policies and procedures including CDD measures (see sections 4 and 6);
6. how to manage transactions on a risk based approach and identify high risk customers and/or high risk behaviour(see section 6);
7. how to report suspicious activity to the MLRO;
8. the penalties for committing offences under POCA and related legislation; and
9. relevant data protection requirements.

It is essential to also train employees to understand how money laundering and terrorist financing schemes could take place through the business by providing examples of this.

9.2 How often does training need to be given?

Employee training must be an ongoing exercise which is regularly under review. Risk assessments and polices must be regularly updated and circulated to members of staff.

9.3 Records

HVGDs must keep a staff training record to demonstrate to the OFT that its staff are aware of the business's AML/CFT policies and procedures (see section 8).

9.4 What responsibilities do employees of HVGDs have?

Employees of HVGDs must:

1. know who the MLRO is and what the MLRO's role is;
2. be able to detect suspicious activity and report it to the MLRO;
3. be aware of the steps taken by the business to ensure it is not used for ML/TF;
4. have access to and familiarise themselves with all of the business's AML/CFT policies and procedures; and
5. be aware of the penalties for committing offences under POCA and related legislation.

It is the responsibility of the HVGD to provide adequate training to its employees (see section 9.1 and 9.2).

10.Potential High Value Goods Dealers

10.1 Who are Potential HVGDs?

Potential HVGDs are dealers in goods which have not yet received a payment in cash above the monetary threshold but are open to accepting such cash payments.

10.2 Why do Potential HVGDs have obligations?

Potential HVGDs need to be prepared for the moment that they do receive large payments even if this has not yet happened. As soon as the business receives a payment above the monetary threshold it will automatically be a HVGD and these guidance notes will be applicable to that business in full.

10.3 What are the obligations of Potential HVGDs?

Potential HVGDs' obligations include, but are not limited to:

1. Carrying out a risk assessment of the business's attractiveness and vulnerability to ML/TF (see section 3);
2. Establishing appropriate AML/CFT policies, controls and procedures commensurate to the business's ML/TF risks (see section 4);
3. Appointing a MLRO who understands the business's ML/TF risks, is acquainted with POCA and who shall be responsible for all AML/CFT matters (see section 5)
4. Keep records of transactions involving high value goods above £2,000 (see section 8.4); and
5. Training staff to ensure they are aware of the HVGD's ML/TF risks and of the business's AML/CFT polices (see section 9).

References to HVGDs in Sections 3 to 9 of these Guidance Notes should be read, where relevant, as also applying to Potential HVGDs.

10.4 Can a Potential HVGD avoid these obligations?

Yes. A dealer need not comply with the obligations in these guidance notes at all if:

4. they are not a High Risk Dealer (see Section 11 below);
5. they have a written policy not to accept cash payments above the monetary threshold; and
6. they have notified the OFT of their no cash policy.

11.High Risk Dealers (HRDs)

11.1 What is a High Risk Dealer (HRD)?

High Risk Dealers are businesses that:

1. are not HVGDs because they have not received a payment above the monetary threshold, but
2. are dealers in goods which are considered to have a higher inherent risk and vulnerability to ML/TF (see 11.2 below).

Despite not being HVGDs these businesses are required to have AML/CFT measures in place due to the nature of the goods they trade even if they are not accepting cash payments above the monetary threshold.

11.2 Which businesses are HRDs?

Businesses that are dealers in the following high value goods are considered HRDs:

1. jewellery and precious metals & stones, to include watches;
2. motor vehicles requiring registration under the Traffic Act;
3. marine craft and nautical equipment;
4. art, artistic works and antiques; and
5. arms, ammunition and explosives,

together, the **high risk goods**.

11.3 What are the obligations of a HRD?

HRDs must apply the general AML/CFT principles of these guidance notes to all its cash transactions for high risk goods. In particular, HRDs should:

1. Carry out a risk assessment of the business's attractiveness and vulnerability to ML/TF and provide a

written ML/TF risk assessment to the OFT (see section 3);

2. Establish appropriate AML/CFT policies, controls and procedures (see sections 4 and 11.4);
3. Appoint a MLRO who understands the business's ML/TF risks, is acquainted with POCA and who shall be responsible for all AML/CFT matters (see section 5);
4. Keep records of transactions involving high risk goods above £2,000 (see section 11.4).; and
5. Train staff so they are aware of the business's ML/TF risks and the business's AML/CFT polices (see section 9).

11.4 Keeping record of high risk good sales

The OFT requires all HRDs to collect the following data in relation to every cash transaction above £2,000 for any high risk goods (see section 11.2):

1. a detailed description of the good(s) sold;
2. the quantity of the goods sold, by unit or otherwise (e.g. weight);
3. the relevant serial number for the goods;
4. the full name of the person purchasing the goods as stated in their passport/ID;
5. the cash paid in exchange for the goods; and
6. an identifying reference for the goods to the HRD's stock records.

This may be kept in the form of a detailed invoice.

HRDs must regard all transactions in cash for high risk goods by a person, or group of associated persons, as a series of linked cash transactions for determining whether they cumulatively go above £2,000

11.5 What policies need to be put in place?

The AML/CFT policies implemented by HRDs, including how they carry out their risk assessments on their customers and related transactions, needs to be appropriate and proportionate to mitigate the inherent risks of trading in the relevant high risk goods. HRDs will be required to assess all of their cash transactions and clients more generally than HVGDs to determine what policies are appropriate to ensure that their business is not used for ML/TF.

11.6 Reporting suspicious activity.

Where a HRD's MLRO identifies suspicious activity they must report it to the GFIU as specified in section 5.8.

12.Reporting Ownership & Management Changes

12.1 HVGD and HRD reporting requirements.

HVGDs and HRDs are required to report to the OFT where there is a change to the ownership or management.

12.2 What changes must be reported?

The OFT must be notified of a change to:

1. the BO of a HVGD or a HRD, including, but not limited to shareholders, partners and silent partners;
2. the board of directors, an executive and/or another senior manager of a HVGD or a HRD;
3. a person holding or appearing to the OFT to intend to hold a management function

in a HVGD or a HRD; and

4. a person in accordance with whose wishes or directions any person involved in the carrying on of the business of a HVGD or a HRD acts or it appears to the OFT will act.

12.3 When do I need to report the change?

The OFT must be notified in writing within seven days of the relevant change.

12.4 What will the OFT do with the information?

Upon receipt of a notification the OFT shall conduct a fit and proper assessment of that person.

13. Useful Contacts

13.1 Gibraltar Financial Intelligence Unit

The Gibraltar Financial Intelligence Unit (GFIU) receives, analyses and disseminates financial intelligence gathered from Suspicious Activity Reports.

Suite 832, Europort, Gibraltar

Tel: (+350) 20070211

Fax: (+350) 20070233

gfiu@gcid.gov.gi

www.gfiu.gov.gi

13.2 HM Customs Gibraltar

HM Customs Gibraltar is the supervisory authority for the trade in tobacco in Gibraltar.

Customs House, Waterport, Gibraltar

Tel: (+350) 20078879/20079988

Fax: (+350) 20049278

financial.investigations@hmcustoms.gov.gi

www.hmcustoms.gov.gi

Schedule 1 – How to Identify Customer ML/TF Risks

1. Identifying risk factors

This schedule sets out a number of common factors that HVGDs and their employees may take into account when carrying out a ML/TF risk assessment of a customer or a transaction.

For assessing a HGVD's ML/TF risk please refer to section 3.

It is important to note however that these are only indicators to consider when assessing risk. The identification of one of these factors need not necessarily mean that ML/TF is, or will be, taking place. They will however assist the HVGD and its employees in applying the risk based approach and ultimately deciding whether the activity, when considered with the rest of the information at their disposal, is suspicious.

The factors listed in this schedule are not an exhaustive list and HVGDs and their employees should take into account all of the information at their disposal to determine if there is ML/TF risk. If more information is required it should be requested before proceeding with a transaction to ensure that there is no ML/TF risk.

2. Assessing low risk customers?

Pursuant to Section 16 (3) and (5) POCA, when assessing the risks of ML/TF relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, a HVGD must take into account at least:

1. the factors of potentially lower risk situations set out in Schedule 6 POCA; and
2. the risks identified within any information that is made available to the HVGD pursuant to the National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing Regulations 2016.

3. Who are high risk customers?

Pursuant to Section 17 (4), when assessing the risks of ML/TF HVGDs must take into account at least the factors of potentially higher- risk situations set out in Schedule 7 POCA.

The following are indicators of high risk customers:

1. brand new customers carrying out large one-off transactions;
2. customers engaged in a business which involves the constant movement of significant amounts of cash;
3. customers who carry out transactions that:
   i. do not make commercial sense;
   ii. have an unusual pattern; and/or
   iii. are complex;
4. existing customers where:
   i. the transaction is different from the normal business of the customer;
   ii. the size and frequency of the transaction is different from the customer's normal pattern,

   (see paragraph 6 below).
5. complex business ownership structures with the potential to conceal underlying beneficial owners;
6. politically exposed persons (these will always require enhanced CDD, see

section 6.12 of the guidance notes and paragraph 4below); and/or

7. persons from high-risk jurisdictions (a list of these can be found on the Financial Action Task Force (**FATF**) website: http://www.fatf-gafi.org).

4. Who are politically exposed persons?

A politically exposed persons (**PEP**) is defined in section 20A POCA as a person who is or has been entrusted with prominent public functions and includes the following:

1. Heads of State, heads of government, ministers and deputy or assistant ministers;
2. Members of parliament or of similar legislative bodies;
3. Members of the governing bodies of political parties;
4. Members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
5. Members of courts of auditors or of the boards of central banks;
6. Ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
7. Members of the administrative, management or supervisory bodies of State-owned enterprises; and
8. Directors, deputy directors and members of the board or equivalent function of an international organisation.

(Note however that middle-ranking or junior officials carrying out a public function referred to in 1 to 8 are not regarded as PEPs).

These individuals, who may be local or international PEPs, are usually at a higher risk of having possible connections to money laundering in particular due to the position and influence they hold and will require enhanced due diligence. This also includes the PEP's 'family members' and 'persons known to be close associates' (see definition in section 20A POCA).

For more information about transacting with PEPs see section 6.12 of the guidance notes.

5. What is high-risk behaviour?

The following are indicators of high-risk behaviour:

1. an unwillingness to produce evidence of ID or the production of unsatisfactory evidence of ID;
2. where the customer is, or appears to be, acting on behalf of another person, an unwillingness to give the name(s) of the person(s) they represent;
3. an unwillingness to disclose the source of funds;
4. suspicion about the source of funds disclosed e.g. does not tally with type of individual;
5. multiple purchases of the same high value goods which are normally only bought once by other customers;
6. an unusually big cash or foreign currency transaction for the goods purchased;
7. a willingness to bear very high or uncommercial penalties or charges;
8. no apparent reason for using your business's services, e.g. another business is better placed to handle the transaction;

9. situations where the customer's source of funds are unclear; and/or
10. the unusual involvement of third parties particularly where the customer appears to have a low income.

6. Monitoring patterns of business.

Risk assessments must also include the review and monitoring of business patterns and unusual transactions. Monitoring these business patterns is essential to the implementation of an effective risk-based approach, for example:

1. a sudden increase in business from an existing customer;
2. uncharacteristic transactions which are not in keeping with the customer's financial situation;
3. the pattern of an existing customer has changed since the business relationship was established;
4. there has been a significant or unexpected improvement in an existing customer's financial position and the customer can't give a proper explanation of where money came from;
5. peaks of activity at particular locations or properties; and/or
6. unfamiliar or atypical types of customer or transaction.

7. Enhanced due diligence and reporting.

The indicators above may, when assessed by the HVGD or its employees, require enhanced due diligence to ensure that the AML/CFT risk is understood appropriately and the necessary risk assessment is carried out (see section 6.9 of the guidance notes).

If the HVGD's MLRO, having considered all the factors surrounding the customer and the transaction, knows or suspects that ML/TF is taking place, they should submit a suspicious activity report (see sections 5.6 to 5.8 of the guidance notes).

Schedule 2 – Glossary of Terms & Abbreviations

AML/CFT	Anti-money laundering and countering the financing of terrorism
BO	Beneficial owner
Cash	Money in coins or notes.
CDD	Customer due diligence
FATF	Financial Action Task Force
GFIU	Gibraltar Financial Intelligence Unit
HVGD	High-value good dealer
HRD	High risk dealer
High risk goods	Refer to section 11.2
High value good	Refer to section 1.5
ID	Personal identification document
ML/TF	Money laundering and terrorist financing
MLRO	Money laundering reporting officer
Monetary threshold	Refer to section 1.6
NRA	National risk assessment
OFT	Office of Fair Trading
PEP	Politically exposed person
PF	Proliferation financing
SAR	Suspicious activity report